Department of Defense Bloggers Roundtable With Eric Rosenbach, Deputy Assistant Secretary of Defense for Cyber Policy, and Richard Hale, Deputy Chief Information Officer for Cybersecurity Via Teleconference Subject: The Pentagon's Recent Initiatives to Improve Defense Industrial Base (DIB) Network Defenses and Allow DIB Companies and the Government to Reduce Damage to Critical Programs When Defense Information is Compromised Time: 12:30 p.m. EDT Date: Monday, May 14, 2012

(Note: Please refer to www.dod.mil for more information.)

WILLIAM SELBY: I'd like to welcome you all to the Department of Defense Bloggers Roundtable for Monday, May 14th, 2012. My name is William Selby with the Office of the Secretary of Defense Public Affairs, and I'll be moderating the call today.

We are honored to have our guests Mr. Eric Rosenbach, deputy assistant secretary of defense for cyber policy, and Mr. Richard Hale, deputy chief information officer for cybersecurity. They will be discussing the Pentagon's recent initiatives to improve defense industrial base network defenses and allow the defense industrial base companies and government to reduce damage to critical programs when defense information is compromised.

A note to the bloggers on the line today. Please remember to clearly state your name and organization in advance of your question. Respect our guests' time, keeping your questions succinct and to the point. And please, we ask if you are not asking a question that you please keep your phone on mute.

Has somebody else just joined us?

Q: Yes, this is Sharon Weinberger.

MR. SELBY: Thanks, Sharon. You are eighth on the line. And we just got through our opening statement from me.

And Mr. Rosenbach or Mr. Hale, if you have opening statements, the floor is yours.

RICHARD HALE: Hi, this is Richard Hale. I just wanted to give a little bit of background on what both of us are going to describe today. A bit more than four years ago, the Department of Defense started a program to better protect DOD information that sits in the defense industrial base companies' networks. And the idea behind the program was to share unclassified and classified government information that can help these companies protect DOD information better.

The program -- the idea with the program was that it was going to be completely voluntary, companies could join if they wanted. And then a second important idea in the program was that companies, again on a strictly voluntary basis, could report cyber incidents back to the department, including could share malware that's found on their company's systems, with the government, government would analyze that and then push back out to the participating defense industrial base companies and push back out to the rest of the federal government any threat information that could be derived from that, including signatures that could go right into defenses or a cyberattack detection and diagnosis systems.

So that defense industrial base cybersecurity program, again, has been in operation for a bit more than four years. There are 36 companies participating in it.

And then a few years ago, the DOD began an effort to see whether there were other models or to develop other models for sharing, again on a voluntary basis, with the industry. And an enhancement to the defense industrial base program was developed. And Eric Rosenbach is going to talk about that enhancement.

But the enhancement was to share unclassified and classified threat signatures with commercial service providers with with ISPs who could then provide protection to the defense industrial base companies by using these signatures.

So this is all one program, but there are two core components to it.

The main defense industrial base cybersecurity program had been capped at 36 companies until the DOD published a rule in the Federal Register. The rule is approved by the Office of Management and Budget and was published last Friday. So what that means is the program can now expand to more companies. The eligible companies are cleared defense contractors that have facility clearances because they have to be able to handle classified information. They have to be able to have a node on this sharing system called DIBNet.

And the way a company gets into the program is they go to our website at DIBNet.dod.mil, and they download program information and a copy of something called the framework agreement which is the instrument that we use to lay out roles and responsibilities between the government and the company.

And then the company, once they've executed that and they've been approved, we put DIBNet in at the company. We work with -- you know, that can take a bit of time. And then we begin this sharing.

Optionally then, the company can execute an amendment to the framework agreement to participate in the commercial service provider part of the program.

And I think that's all I want to say as an opening statement. And I'll turn it over to Eric Rosenbach.

ERIC ROSENBACH: Good afternoon. This is Eric. I'll just try to be real quick.

As I think you may have seen from some of the other press reports and our press release, on Thursday that interagency and the White House approved us to make permanent and expand a pilot program, which is part of the larger program that Richard just spoke about, that involves using specialized intelligence information, working through DHS and providing it to Internet service providers to scan incoming Internet traffic to select member of the defense industrial base.

Just a real quick reminder about why we were trying to do this. The defense industrial base companies face a kind of unrelenting attack from sophisticated actors who are trying to steal intellectual property and sensitive defense information. And we wanted to try to do something to address that more-sophisticated threat because the defenses of everyday firms may not necessarily be a -- (inaudible) -- to defend against those.

So I told you a little bit about how it works, and you can ask more questions if you have details about that. But it's probably also interesting to say why we're doing this and kind of where we want to go.

This model, from both the legal, technical, operational and policy perspective, is something that we invested a lot of work in. And that involves different actors, including DOD intelligence community, the Department of Homeland Security and the Internet service providers. It's something that we're pretty proud of, and I think offers the potential to have not only a model of support for the defense industrial base and the Department of Defense, but possibly, if this is where the interagency and the White House decides, protection of critical infrastructure.

So you can see it may play an important role in the strategic defense of the country in the way that I like to think about it.

MR. SELBY: Thank you very much, sir.

And once again, I think there was some background noise there. I'm not sure. But please make sure your phone is on mute while the speakers are talking.

Chuck, you were first on the line, you can go ahead with your question.

Q: Good morning, gentlemen. Chuck Simmins with America's North Shore Journal. Thank you for participating with us today.

One quick question and one that might be a little bit more complicated. How many firms are estimated to be eligible for this new program, not participating, but eligible?

And can you describe the relationship of this program to Cyber Command, and what you're doing to avoid violations of the Posse Comitatus Act? Thank you.

MR. HALE: This is Richard Hale. Eric and I will both answer this one.   We believe that there are roughly 8,000 defense industrial base companies that are eligible for the program. We aren't sure how many will choose to join. Again, it's completely voluntary. But we're estimating that the program could grow to as many as 1,000 companies. But if it grows to more than that, we would be pleased.

So with that, I will turn over the second question to Eric Rosenbach.

MR. ROSENBACH: Hello, Chuck. Your question is on how we ensure that it doesn't violate posse comitatus. And this one is actually pretty easy because the Department of Defense isn't actually operating domestically in any way in this case.

So some of the information that's collected from DOD intelligence organizations is passed to the Department of Homeland Security to check over it, make sure there's nothing there in particular that would violate civil liberties, Fourth Amendment concerns. Then passed from DHS, who has the lead for the relationship with Internet service providers, to the Internet services providers where they scan the traffic.

All of this is done with the consent of the companies. So it's completely voluntary to join the operation, and it's also completely voluntary, you know, to withdraw. Any information exchanged is all done on a voluntary basis.

Q: Thank you, sir.

MR. SELBY: And Michele Cowell, you are next.

Q: William, I think I'm going to pass just momentarily and come back around.

MR. SELBY: Sure. OK.

Sandra?

Q: Thank you. Good afternoon. Sandra Erwin with National Defense. I wanted to ask either one of you about the issue of adding classified information into this program. Are we to assume that there is increased concern about the classified information potentially being compromised? And if that's the case, what countries or what organizations are you aware of that have the capability to access classified information?

MR. HALE: So the -- this is Richard Hale. The way the program works is that the companies who get classified from the government have to protect it to the same level that the government protects that classified information. So they have to have the appropriate personnel security. They have to have the appropriate physical security. And they have to have the appropriate cybersecurity. So there isn't any difference in the way the companies that get this information have to protect it than the way the government has to protect that information.

The defense industrial base cybersecurity program is focused on, as Eric Rosenbach said, is focused on the protection of Defense Department information primarily on classified information. Although it may be sensitive information, it's certainly intellectual capital of the department and of the companies. So we're working to protect that unclassified information from compromise by people who might want to steal that information for various reasons.

Q: But I'm sorry, I thought that the intent of enhancing this program was to share more classified information with the industrial base. And that sort of my question was, does that mean that you'll have increased concerns about classified information being stolen potentially by hackers or whoever?

MR. ROSENBACH: This is Eric Rosenbach. So in the enhanced part of the program, despite the fact that we're making more widespread use of classified information, which is classified signatures as they're known, because the signature base is actually centralized in DHS and then the Internet service providers, and the Internet service providers have to have something that's known as a skiff (ph) -- it's a secure facility where you can hold classified information and meet all the standards laid out by DOD -- it's actually less likely that it would leak or that the intelligence agencies of another country could get to it because it's held in fewer places.

So again, it's something that kind of shows the advantage of the model, is that we can provide enhanced service or the information for an enhanced service to the ISPs, but we don't have to necessarily pass the information itself on a more widespread basis. We're just using the power of the network and the Internet itself to try to provide a little bit of additional protection.

Q: OK. Thank you very much.

MR. SELBY: And Phyllis, you were next.

Q: Yes. Phyllis Zimbler Miller, mrslieutenant.blogspot.com. I'm a little confused because, as Mr. Hill talked about, unclassified information being protected from people who might want to steal it. Since it's unclassified, they can probably get it any other way. So could you kind of give us a scenario of an example where they couldn't get it another way, even though it's unclassified, but how this cybersecurity system would protect it?

MR. HALE: So this is Richard Hale. The unclassified information that these companies often hold on our behalf is still potentially information that is not publicly available. So even though something -- so this might be information that is marked for official use only, for instance. Some of this information may be company proprietary information in addition to that. So there are still controls on the information that are used by the company and by the government to ensure that the information is not made available to everybody. So this is not stuff that would be put up on a website that the general public could get to, for instance.

So what the program and the enhancement of the program are both after is keeping those controls around that information in tact in the face of people who want to breach the control system that we, the government and the companies, have put in place.

Q: Thank you.

MR. SELBY: And Gail.

Q: This is Gail Harris with the Foreign Policy Association. I was wondering, if it's your hope that if we have continued success with this program, as we did the earlier, obviously, iteration, that this will lead to a more comprehensive policy which will be able to defend our critical infrastructure. My understanding is, unless we can develop a comprehensive strategy, then there's still a major vulnerability for cyberattack or in case of a cyberwar, cyber Pearl Harbor type scenario.

MR. ROSENBACH: Hey, Gail, this is Eric Rosenbach. That's a really good question. And that's a little bit what I was hinting at when I said I think the model is something that could be used to scale to protect critical infrastructure as well.

But I want to be very clear, that's not a decision that we at the Department of Defense would make. That's something that would be led by the White House, and the Department of Homeland Security would have the lead, the lead for domestic cybersecurity.

But the advantage of the model is that because it's done on the network and by the companies that provide the Internet service to even the critical infrastructure, you have a lot of flexibility for scaling it and using these enhanced measures.

It's kind of unrealistic, I think, in this day and age to think of putting government-built boxes that would scan the network and protect the entire country, just because it's technically almost certainly unfeasible, and there are a lot of civil liberties and privacy concerns that I think would probably keep that from happening, too.

So you know, it's promising, but we have to see how everything goes.

Q: All right. It's my understanding, though, if we don't come up with a solution where we get a sense of what's happening on the network, we would not be able to identify what is just a cyberhack against a particular company and what might be a larger-scale cyberattack in terms of warfare against the United States.

MR. ROSENBACH: Here's one way to think about that, is that there are different places along the architecture of the Internet where you might be able to see an attack coming. One is at the border of individual firms or the critical infrastructure network where there's kind of a perimeter defense.

One -- another might be at the border of the nation of the United States or other countries where you could look at this.

And then using intelligence mechanisms, there are other places out in cyberspace where you may be able to see an attack either being perpetrated or planned.

So we don't want to rely just on one specific solution. And this is the one that would most likely help somewhere in between the national borders and the borders of specific firms.

But you know, you have to be realistic, too, about the Internet and the volumes of data you're talking about. Right now it's, I would say, pretty hard to understand how you would see all Internet traffic for the nation and scan it, even if there were a policy or legal decision that you could do that. So you have to try to invest in the best risk-mitigation factors as you can and do other things in national security to try to lower the risk to the country for that type of attack you're talking about.

Q: Right, I understand. The issue for me has always been that there is an issue that some companies are reluctant to bring up that they're under attack. So if you're trying to figure out, again, if something is just an isolated incident, a criminal-type activity, versus a larger-scale thing, unless we can have a more-comprehensive policy where people report the things, then we're still going to have gaps in our coverage.

MR. ROSENBACH: Again, that's a great point. I can tell you're an old intel officer, and you know what you're talking about.

Q: (Chuckles.)

MR. ROSENBACH: But I'd say one of the other things that we're trying to push forward is the legislation that's on the Hill right now in the Senate. The Lieberman-Collins bill has provisions in there that have requirements for people to report when they've been hacked. So it would be very helpful in getting more of that forensic evidence that helps the government understand what's going on.

And so that's, you know, just kind of a basic starting point, as you mentioned. The team is kind of unbelievable to some folks who haven't really spent a lot of time in this space. That firms now don't even necessarily have to report that they've been hacked or attacked.

Q: Thank you.

MR. SELBY: And on to Jared.

Q: Hi, thanks for doing this guys. First, just a clarification on the time line. Richard said at the beginning of the call, I believe, that this has been under way for four years, which that's the first I've heard that this is more than about a year old. The first time I became aware of the cyberpilot was when Secretary Lynn announced it last June. Am I conflating two issues?

MR. HALE: So the program to work with the defense industrial base companies and share classified and unclassified threat intelligence with them has been going on for a bit more than four years. The pilot that Secretary Lynn announced is the one that is the part of the program that Eric has been talking about. And it's the part that says -- it's the part that's focused on using the ISPs or commercial service providers of some sort to provide the protection as a service as opposed to sharing the classified information directly with the defense industrial base company and then expecting the company to use that information to protect itself.

So these are both parts of the same program. The second part, the ISP/commercial service provider part of the program is the part that's about a year old.

Q: Gotcha. OK. And then with regard to the ISPs, do they already have skiffs (ph) up and running and have cleared security personnel that are able to handle this information? Just because it sounds -- it seems kind of like a nontraditional role, in my mind, for ISPs, at least the way that I think about what they do. And how many ISPs are we talking about?

MR. ROSENBACH: Right now there are three ISPs that are up and operational. And all three definitely have skiffs (ph). In order to participate in the program, particularly as a service provider, you have to meet all of the DOD and intelligence community requirements to have a skiff (ph) and handle classified information.

And you're right, it is -- it's untraditional that the Internet service providers play this role. And that, again, kind of shows the value of the model. It is something new, and it is a new type of collaboration between the government and the private sector, and I think one of the only ones that I've ever seen anyway that provides operational value in terms of mitigating the risks for firms.

So we don't say that this is a silver bullet for cybersecurity and that it will prevent all attacks, but it does provide additional measures of risk mitigation. And that's what we think we need to keep working on and expanding. Q: If I could sneak one more in here. During the pilot phase, was this more of a proof-of-concept kind of thing? Or can you point to instances where a serious incident or intrusion was actually stopped or mitigated, understanding you probably can't provide too much detail?

MR. ROSENBACH: You know, honestly, I would say that it was both, that it was definitely a proof-of-concept, and we saw over the course of the one-year pilot period that efficacy of the operation really improves towards the end when we had better procedures in place, we had a more specialized signature set in place. And that then resulted in more operational successes in blocking the type of advanced, persistent threat actors that, you know, this was all designed to defend against.

So I can't unfortunately speak in too much detail about those, but there definitely were successes. And one indication, I think, of the value of the program, this aspect of the overall program, is that it is on a pay-for-service model, and the Internet service providers are now offering it as a paid service. And they have clients coming in, so you have to think that that's one indication of value, anyway, not the silver bullet, again, but definitely one indication that it's mitigating some of the risks these firms face.

Q: And those clients can be anybody, they don't have to be DIB companies?

MR. ROSENBACH: No, right now they do need to be DIB companies. And they also need to be members of the overall program. So they enter in through the program that Richard talked about, and then they can opt in for this enhanced part of the program.

Q: OK, thank you.

MR. ROSENBACH: Thank you.

MR. SELBY: And Zach, please.

Q: Hi, Zach with Defense News. You mentioned a little bit about the improvements in the effectiveness of the program -- (inaudible). A lot of what I've heard about from the companies is that the trust increased, both in their willingness to share information on threats and in their feelings over getting better intelligence back in the other direction.

But there's a lot of concern with the movement over to DHS, that that trust relationship will continue. I just want to ask, how do you think you'll be able to maintain that trust relationship or improve it as you expand the program and include more (ears ?) into the information that's being shared, and have DHS running the program as opposed to DOD?

MR. ROSENBACH: That's a really good question because we often say around DOD and the interagency, the hardest part of getting this up and running was the soft stuff, which is relationships, trying to figure out the policy and some of the law. And there are two trust relationships that really improved over the course of the program.

The first, just to be candid, is the trust relationship between DHS and DOD. And we're at a point now that we really are back-to-back and work very closely together. And the roles that we've designed in the program, I think, are quite good, where DHS has the lead with the Internet service providers, but DOD maintains the lead in working with the DIB companies. And that's working very well.

The other is the relationship between the firms -- either the Internet service providers or the DIB companies -- and DOD and DHS. And I'm going to let Richard talk a little bit more about that.

And I would just say one final thing about DHS is, their capacity as an organization and their leadership has really improved dramatically. And I think that they get a somewhat unfair, bad rap for not being able to do a lot of the things in the cybersecurity space that are expected of them. And I think that that reputation is unfair. They're making quite strong improvements and, you know, really are equal partners in this cybersecurity arena.

MR. HALE: OK, so this is Richard Hale. What I'd say is, over the course of the four years that the overall program has been running, we've built up trust over time the way you often build up trust. The companies found that by reporting incidents voluntarily, they got value back because they were getting then those incidents processed -- or incidents from all the companies processed and pushed back out to the companies, so their defense is improved the more they reported and the more their peers reported.

That built up a lot of the trust, I think, that we needed to have in place in order to then work the enhanced part of the program, which is the ISP-based part of the program.

We will continue to work. We have regular meetings with the companies where they give us feedback on all aspects of the program. And we will continue to do that as we expand the program. And we do listen to them, again, on all aspects of this. And all aspects of this sharing are going to evolve, right?

We don't know how to defeat the cyberthreat yet by this sharing. And as Eric said, it's a piece and a really important piece of an overall cybersecurity strategy for the companies or for the DOD or for the government.

I just want to foot stomp one thing. To get into this defense industrial base cybersecurity program and to participate is free. To participate in the enhancement is not necessarily free. The cost is going to be or the price is going to be set by the participating Internet service providers or commercial service providers who are providing the service in the enhancement. Q: Thank you, gentlemen.

MR. SELBY: And Sharon Weinberger.

Q: Yeah, just a very brief question. You had mentioned that three Internet service providers are now participating in the enhanced program. Is that correct? And if so, which ones are they?

MR. ROSENBACH: That is correct. But we prefer not to name individual, specific firms. Just that's their preference.

Q: OK. Thank you. Could you just talk for a second about then, for those firms that are participating, what exactly is it that they -- what information do they provide to the DOD? And then what -- just information on threats, or can you just expand on that a little bit?

MR. ROSENBACH: Just if I could clarify your question, what information do they Internet service providers provide to DOD?

Q: Yes.

MR. ROSENBACH: Well, so there is some reporting information, again, remember voluntary, that could come from the participating DIB companies. From the Internet service providers, the information goes to DHS, not directly to DOD. Again, they have the lead with Internet service providers and will look at it.

The type of information that might go back would certainly not be PII, personally identifiable information. It would be more technical information that would help understand whether or not the signatures were correct, whether they were helpful, whether they had hit or not.

Q: So does that mean it's stripped of the personally identifying information, or are there procedures in place to do that?

MR. ROSENBACH: Yeah, that's exactly right. There are very rigorous procedures in place to minimize the information to begin with and to definitely strip anything that would be considered PII.

The privacy/civil liberties aspect of this has been really in the forefront of our minds throughout the entire pilot. And you know, we have very rigorous SOPs in place, but then also additional checks and balances just to make sure that any of the information that might come back to the government is done with full consent and it is done on a completely voluntary basis. And then also, it is subject to all of the things I just told you about in terms of looking for civil liberties.

The program has been reviewed by the Department of Justice and also by a lot of the privacy experts within the U.S. government.

Q: OK, thank you. MR. SELBY: And let's see, Jim -- (inaudible) -- also had joined us.

Jim, did you have any questions?

Q: Yeah, a couple of ones. First of all, I'd like to go back to Mr. Hale's estimate that as many as 8,000 DIB companies are eligible for the program. I had been given a much lower figure of over 2,000. I wonder if you can explain that discrepancy.

Is it over 2,000 are already cleared contractors versus a potential universe of 8,000 that might eventually be cleared just for classified information on their networks?

MR. HALE: So Jim, I'm not sure I can resolve the discrepancy. We think that -- and it may be partly -- (inaudible) -- the number of -- are we still on? Is somebody still on?

MR. SELBY: I still -- I still hear you, sir. I think somebody, one of the callers just must have dropped off.

MR. HALE: OK. It sounded like the call hung up.

We did an informal estimate, and our estimate is not necessarily a rocket-science estimate about what the total universe of companies that might be able to participate would be. And again, what we did was try to figure out what companies had cleared people and what companies had cleared facilities, because those were the two prerequisites for participation.

Some of those companies may be subsidiaries or divisions of other companies in our count, and some of the companies may have merged with some other companies in our count. But we think it's more than 2,000.

Q: (Inaudible) -- responsible about that. Is more than 2,000 indeed the number of companies that are already eligible to participate because they're already cleared Pentagon contractors? Or are there as many as 8,000 that are already cleared?

MR. HALE: We think there could be as many as 8,000 that are already cleared and could be participants in the program.

Q: I see. And does the 2,000, the more than 2,000 level, apply in any way to a separate subset of that larger group?

MR. HALE: I don't think so. What we're trying to estimate, and again, it's an estimate, is how many companies are able to participate, meaning that they've already got -- they meet the prerequisites. And then we're trying to estimate how many will participate. And that one we are very uncertain about. So we're hoping that we get up to 1,000 companies participating, but we don't know what that's going to be. It's up to the companies. Again, it's a voluntary program. Q: Can you describe where the matter stands in the first go- around of companies showing interest or the ones that have been knocking at the door previously? How many seem ready to jump onboard now that the door has been opened to a larger group?

MR. HALE: So we have 36 companies that are in right now, and they're very active participants in the program. And again, 17 of those companies are participating in the enhanced program as well. So we have pretty vigorous participation.

We have, over the course of the last several years, had more than 250 companies express interest in participating in the program, and so we sent email to all of them. So we've kept points of contact for all those companies. We've sent email to all of them on Friday when the program opened, and we started to see responses back already on Monday from some of those companies.

So we think that there is some pent-up demand for participation, but I think it's too early to tell how fast companies are going to ramp up and actually apply for the program.

Q: OK. One last question, if I may.

MR. SELBY: Jim, we've got to -- Jim, we might be able to come back to you in one second. I've just got to make sure I can get everybody in. Let me make sure.

Michele, are you still on the line?

Q: I am indeed.

MR. SELBY: Did you have a question.

Q: Just a real quick question, if I may.

MR. SELBY: OK.

Q: Back in February -- you alluded to the legislation that was on Capitol Hill right now, with respect to the individual states that do not have to report any of the information or -- again, I'm assuming these are the ones that are part of the 8,000 that are voluntary -- has that legislation, is that incorporating that also, mandating the states themselves (take ?) the companies to report?

MR. ROSENBACH: Now, just to clarify -- this is Eric -- that's a good question. Just to clarify, there are two proposals on the Hill that have to do with this. One which was in the White House's original proposal for cybersecurity, but is not clear whether or not it will pass, is to have a federal standard for data breach notifications. As it stands right now, I think there are something like around 45 different state laws on data breach notifications, which is kind of onerous on firms and their general counsels trying to figure out when they need to report information about what standard. So the hope was to set one.

What is in the Lieberman-Collins bill is a provision that says, you know, within a certain context, you have to disclose the fact that you have been hacked or you've been attacked, to the federal government if you're a part of certain critical infrastructures. And that's the part that we find very helpful.

And it wouldn't necessarily put any onus on the states. It wouldn't put onus on the states. It would be for individual firms, not state governments.

Q: And this is in concert with the same dynamic that Secretary Panetta was discussing when they had their press conference with China to get their -- to join us as far as our U.S. cyberspace is concerned, on the same level?

MR. ROSENBACH: You know, I'm not sure I understand exactly. Could you repeat that part of the question?

Q: When they wanted to bring the United States Cyber Command into play with China to have them begin discussions to join in the efforts on the cyberattacks. That was just recently within the last week.

MR. ROSENBACH: Right. No, that's actually a little different. The idea that Secretary Panetta has, which is excellent, is that we want to be able to have a direct relationship with the Chinese military and the People's Liberation Army, in particular, to be able to talk about operations in cyberspace and cybersecurity. We think that's very important because cyberspace is pretty complicated, and we really don't want a misunderstanding to escalate into something that could be a bigger national security threat.

So the idea there is that we really just want to promote more mutual understanding through a direct-type relationship --

(Cross talk.)

Q: -- reporting also.

MR. ROSENBACH: Yeah, that probably would -- it would probably grow into more real-time reporting, which is something that we're working on with other countries right now. But I suspect it may take a little confidence-building with the Chinese before we got to that.

Q: OK. Very good, thank you.

MR. SELBY: And we have time for one more follow up. Jim, did you -- Q: Yeah, I had just wanted to ask if you could give any idea of how much -- just the ballpark figure perhaps, the ISPs have been charging their DIB clients for the enhanced service.

MR. ROSENBACH: You know, because we want to be very, very conscientious about not influencing the market dynamics of the opt-in aspect, the enhanced aspect, we don't think it's right for the government to talk about rates and, you know, whether they're good or bad or anything like that.

Q: But how is it that they can profit from a government-provided service? I'm just not clear on that point, how the ISPs can devise profits from a service that wouldn't exist except for a taxpayer-funded aspect of the intelligence production that goes into it.

MR. ROSENBACH: OK, well, there are a couple of ways to look at this. If you start very basic -- and I'll try not to blab on too long here as a policy wonk type. But if one of the things you identify in government is that there is, in economic terms, not that the terms are, you know, failures, there's market failure, which means usually when you do market failure analysis in public policy, it's the best indication that you need some government role to alleviate that.

So the idea here is we're providing information that the government already has, no additional cost to the government, to Internet service providers who do invest their own funds in building the infrastructure, the architecture and delivering the service, right? That's something that costs the firms themselves something.

And by doing this, you kind of alleviate that space in which there previously has not been an ability for the private sector to defend themselves against some of the advanced threat.

So if you're looking at it from a profit perspective, I honestly don't know if they're profiting or how they're profiting and to what degree. All I know is that it's definitely addressing a need in cybersecurity, and even better if we can do it with market mechanisms that don't cost the U.S. government additional funds, either in acquisition or just outright investment.

Q: Well, that's a really interesting answer. Appreciate it. I wanted to just ask you -- we've heard that -- MR. SELBY: I'm sorry, Jim, we're going to -- you can email me, Jim. I can give you my email address offline and I can forward your other question to them. Sorry about that.

So with that, sir, Mr. Rosenbach and Mr. Hale, we thank you for your time today. If you could wrap things up with a few closing comments, that would be great.

MR. HALE: Closing comments -- OK. So this is Richard Hale. Again, my only closing comment really is this, what we believe is a unique public-private partnership and an important one, is open for business for company -- cleared defense contractors who might want to participate. So we encourage them to go to this website which is DIBNet.dod.mil. And I think that was on the press release we've put out. And take a look at the program, and if they're interested, participate.

MR. ROSENBACH: And I would just say real quick to reiterate on that point, we're very excited that a lot of the work that we, the Department of Defense, DHS, the whole of government, working with the private sector have put in over the past year to develop what we think is an innovative model. It's not the silver bullet to stop all attacks against the defense industrial base and prevent the theft of all intellectual property, but it's one additional step in risk mitigation.

We think that it's quite scalable. And really want to press forward with protecting as many of the DIB companies as we can. And think that it's promising in terms of thinking about one possible model for protecting the nation and critical infrastructure down the line.

MR. SELBY: Thank you very much, gentlemen. And thank you to everybody on the line who participated today.

The program will be online at DOD Live where you'll be able to access a story based on today's call, along with first documents, such as the audio file and a print transcript.

Again, thank you very much, Mr. Rosenbach, and also, Mr. Hale, for your time.

This concludes today's event. Feel free to disconnect at this time.

END.